QCM - VRAI - FAUX

QCM

Cocher la réponse exacte.

1. L'entier 5 est un inverse modulo 6 de

☐ 5. ☐ -5. ☐ 1.

2. Soit p un nombre premier.

☐ $p \wedge p^2 = 1$. ☐ $p \wedge p^2 = p$. ☐ $p \wedge p^2 = p^2$.

3. L'ensemble des solutions entières de l'équation $11x - 5y = 1$ est

☐ $\{(1+5k, 2+11k), k \in \mathbb{Z}\}$. ☐ $\{(1+11k, 2+5k), k \in \mathbb{Z}\}$. ☐ $\{(2+5k, 1+11k), k \in \mathbb{Z}\}$.

4. L'ensemble des solutions entières de l'équation $13x - 17y = 0$ est

☐ $\{(17k, 13k), k \in \mathbb{Z}\}$. ☐ $\{(13k, 17k), k \in \mathbb{Z}\}$. ☐ $\{(17+13k, 13+17k), k \in \mathbb{Z}\}$.

VRAI - FAUX

Répondre par vrai ou faux en justifiant la réponse.

1. Soit n un entier.

$n \equiv 0 \pmod{143}$, si et seulement si, $n \equiv 0 \pmod{13}$ et $n \equiv 0 \pmod{11}$.

2. Pour tous entiers a et b,

a. $-3a \wedge 3b = 3(a \wedge b)$.

b. Si $a \wedge b = a \vee b$ alors $a = b$.

3. L'équation $25x - 80y = 3$ admet des solutions entières.

4. Tout entier admet un inverse modulo 14.

5. Pour tout entier $n \geq 2$, $(n-1)$ est son propre inverse modulo n.

Exercices et problèmes

1 Déterminer $a \wedge b$ dans chacun des cas ci-dessous.

1. $a = 558$ et $b = -1235$.
2. $a = 924$ et $b = 990$.
3. $a = -999$ et $b = 888$.
4. $a = 1890$ et $b = -5250$.

2 Calculer $a \wedge b$ et $a \vee b$ dans chacun des cas ci-dessous.

1. $a = 588$ et $b = -1235$.
2. $a = 51$ et $b = -255$.
3. $a = 2n+1$ et $b = n$, où n est un entier non nul.

3 Trouver les valeurs possibles de l'entier a sachant que $a \wedge 180 = 36$ et $|a| < 360$.

4 Trouver tous les couples (a, b) d'entiers non nuls tels que $a \wedge b = 19$ et $ab = 2166$.

5 Montrer qu'il n'existe aucun couple (a, b) d'entiers tels que $a \wedge b = 19$ et $a^2 - b^2 = 490$.

6 1. Montrer que

$2^5 \equiv -1 \pmod{11}$ et $2^5 \equiv 1 \pmod{31}$.

2. En déduire les congruences

$2^{340} \equiv 1 \pmod{11}$ et $2^{340} \equiv 1 \pmod{31}$.

3. Montrer que 341 divise $2^{340} - 1$.

7 La décomposition de 561 en facteurs premiers est $561 = 3 \times 11 \times 17$.

Soit a un entier premier avec 561.

1. Vérifier que a est premier avec chacun des entiers 3, 11 et 17.
2. Montrer que

a. 3 divise $a^2 - 1$.

b. 11 divise $a^{10} - 1$.

c. 17 divise $a^{16} - 1$.

3. En déduire les congruences

$a^{560} \equiv 1 \pmod{3}$, $a^{560} \equiv 1 \pmod{11}$ et $a^{560} \equiv 1 \pmod{17}$.

3. Montrer que 561 divise $a^{560} - 1$.

8 Soit a, b et d trois entiers non nuls tels que $a \wedge b = d$.

1. Montrer que si un entier n divise $4a + 5b$ et $5a + 2b$ alors n divise 17a et 17b.
2. En déduire que $(4a + 5b) \wedge (5a + 2b) = d$ ou $(4a + 5b) \wedge (5a + 2b) = 17d$.

9 Soit a, b et n trois entiers non nuls.

1. Montrer que si d divise a et b alors d divise $a + bn$ et $a + b(n-1)$.
2. Montrer que si d divise $a + bn$ et $a + b(n-1)$ alors d divise a et b.
3. En déduire que $a \wedge b = (a + bn) \wedge (a + b(n-1))$.

10 1. a. Donner une solution particulière de $5x \equiv 1 \pmod{17}$.

b. En déduire les solutions dans $\mathbb{Z}$ de $5x \equiv 1 \pmod{17}$.

c. Donner les solutions dans $\mathbb{Z}$ de $345x \equiv 1 \pmod{17}$.

2. a. Résoudre dans $\mathbb{Z}$ $5x \equiv 2 \pmod{17}$.

b. Donner les solutions dans $\mathbb{Z}$ de $430x \equiv 2 \pmod{17}$.

11 Résoudre dans $\mathbb{Z}$

a. $17x \equiv 1 \pmod{33}$.

b. $17x \equiv -9 \pmod{33}$.

12 Déterminer l'ensemble des couples (x, y) tels que $12x \equiv 30y \pmod{15}$.

Exercices et problèmes

13 Déterminer l'ensemble des couples (x, y) tels que $11x \equiv 99y \pmod{77}$.

14 1. Vérifier que $2015 \wedge 2007 = 1$.

2. Déterminer deux entiers a et b tels que $2007a + 2015b = 1$.

15 1. Vérifier que $391 \wedge 323 = 17$.

2. Déterminer deux entiers a et b tels que $391a - 323b = 17$.

3. En déduire une solution de $391a - 323b = 204$.

16 1. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $97x + 11y = 1$.

2. Soit l'équation $(E) : 97x + 77y = 7$.

a. Donner une solution particulière de (E).

b. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation (E).

17 On pose $u = 2 + \sqrt{3}$.

1. a. Montrer par récurrence que, pour tout entier naturel $n \geq 1$, $u^n = a_n + b_n\sqrt{3}$, où a_n et b_n sont des entiers naturels.

b. Exprimer a_{n+1} et b_{n+1} à l'aide de a_n et b_n.

2. a. Montrer que $a_n{}^2 - 3b_n{}^2 = 1$ et $a_n b_{n+1} - a_{n+1} b_n = 1$.

b. En déduire que $a_n \wedge b_n = a_{n+1} \wedge a_n = b_{n+1} \wedge b_n = 1$.

18 Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ chacune des équations suivantes.

a. $7x - 14y = 5$. b. $5x - 10y = 10$. c. $29x + 58y = 3$.

19 Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ chacune des équations suivantes.

a. $(4x - 3y - 5)(4x + 3y - 1) = 0$. b. $x^2 - 9y^2 = 2$.

20 1. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $(E) : 13x - 8y = 1$.

2. On considère les triplets (x, y, z) de $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ vérifiant le système $S : \begin{cases} 5x + y - 2z = 1, \\ 8x - 9y + 2z = 0. \end{cases}$

Montrer que si (x, y, z) est solution de S alors (x, y) est solution de (E). Résoudre S dans $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$.

21 1. Déterminer deux entiers u et v tels que $9u - 11v = 1$.

2. Soit a, b et x trois entiers. Montrer que si $x \equiv a \pmod{9}$ et $x \equiv b \pmod{11}$, alors $x \equiv 45b - 44a \pmod{99}$.

3. Résoudre dans $\mathbb{Z}$ le système $\begin{cases} x \equiv 6 \pmod{9}, \\ x \equiv 8 \pmod{11}. \end{cases}$

22 Pour tout entier n, on considère les nombres $a = 2n - 3$ et $b = 3n - 1$.

1. Quelles sont les valeurs possibles de $a \wedge b$?

2. a. Vérifier que pour tout n, le couple (a, b) est solution de l'équation $(E) : 3x - 2y = -7$.

b. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation (E).

3. Déterminer l'ensemble des entiers n tels que $a \wedge b = 7$.

23 Soit p, q et u trois nombres premiers.

On pose n = pqu et on suppose que p–1, q–1 et u–1 divisent n–1.

Soit a un entier premier avec n.

1. Montrer que $a^{p-1} \equiv 1 \pmod{p}$, $a^{q-1} \equiv 1 \pmod{q}$. et $a^{u-1} \equiv 1 \pmod{u}$.

En déduire les congruences $a^{n-1} \equiv 1 \pmod{p}$, $a^{n-1} \equiv 1 \pmod{q}$. et $a^{n-1} \equiv 1 \pmod{u}$.

2. Montrer que $a^{n-1} \equiv 1 \pmod{n}$.

3. Décomposer 561 en produit de facteurs premiers et montrer que $224^{560} \equiv 1 \pmod{561}$.

4. Montrer que $561^{1728} \equiv 1 \pmod{1729}$.

24 1. Soit a et b des entiers naturels non nuls tels que $(a+b)\wedge ab = p$, où p est nombre premier.

a. Montrer que p est un diviseur commun de a et b.

b. Montrer que $a\wedge b = p$.

2. On désigne par a et b deux entiers naturels tels que $a \le b$.

a. Résoudre le système $\begin{cases} a\wedge b = 5 \\ a\vee b = 170 \end{cases}$.

b. En déduire les solutions du système $\begin{cases} (a+b)\wedge ab = 5 \\ a\vee b = 170 \end{cases}$.

25 On désigne par x et y deux entiers naturels non nuls tels que $x < y$.

Soit S l'ensemble des couples $(x,\ y)$ tels que $x\wedge y = y - x$.

1. Calculer $363\wedge 484$.

Le couple $(363, 484)$ appartient-il à S ?

2. Soit n un entier naturel non nul.

Le couple $(n, n+1)$ appartient-il à S ?

3. a. Montrer que $(x,\ y)$ appartient à S, si et seulement si, il existe un entier naturel k non nul tel que $x = k(y-x)$ et $y = (k+1)(y-x)$.

b. En déduire que pour tout couple $(x,\ y)$ de S, $x\vee y = k(k+1)(y-x)$.

4. a. Déterminer l'ensemble des entiers naturels diviseurs de 228.

b. En déduire l'ensemble des couples $(x,\ y)$ de S tels que $x\vee y = 228$.

26 Le plan est rapporté à un repère orthonormé direct $(O,\vec{u},\vec{v})$. On considère l'application f qui au point M d'affixe z associe le point M′ d'affixe z′ tel que $z' = \frac{3+4i}{5}\overline{z} + \frac{1-2i}{5}$.

1. a. Déterminer l'ensemble des points invariants par f.

b. Quelle est la nature de f ?

2. a. Déterminer l'ensemble D des points M d'affixe z tels que z′ soit réel.

b. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $4x - 3y = 2$.

c. En déduire les points de D dont les coordonnées sont entières.

3. On considère les points M d'affixe $z = 1+iy$, où $y\in\mathbb{Z}$.

Déterminer les entiers y tels que $\mathrm{Re}(z')$ et $\mathrm{Im}(z')$ soient entiers.

27 Soit a et b deux entiers.

1. Montrer que si $(a^2+ab-b^2)^2 = 1$ alors a et b sont premiers entre eux.

On considère l'équation $(E): (x^2+xy-y^2)^2 = 1$.

2. Déterminer les solutions entières de (E) telles que $x = y$.

3. Soit (p,q) une solution de (E).

a . Montrer que $(q, p+q)$ est une solution de (E).

b. En déduire que $(p+q, p+2q)$ est une solution de (E).

c. Donner six solutions de (E).

28 Le but de l'exercice est déterminer l'ensemble E des triplets (x,y,z) de $\mathbb{N}^*\times\mathbb{N}^*\times\mathbb{N}^*$ tels que $x^2+y^2 = z^2$.

1. Montrer que pour tout couple (a, b) d'entiers naturels non nuls tels que $a > b$, $(a^2-b^2, 2ab, a^2+b^2)$ est un élément de E.

2. Soit (x,y,z) un élément de E tel que $x\wedge y = 1$.

a. Montrer que $x\wedge z = 1$ et $y\wedge z = 1$.

b. Montrer que x et y ne sont pas tous les deux pairs.

c. Montrer que l'équation $a^2 \equiv 2 \pmod 4$ ne possède pas de solution entière.

d. Montrer que si x et y sont tous les deux impairs alors $x^2+y^2 \equiv 2 \pmod 4$. En déduire que x et y ne peuvent pas être tous les deux impairs.

e. On suppose que x est impair et y est pair.

Montrer que z est impair et que z+x et z-x sont pairs.

En déduire qu'il existe deux entiers strictement positifs p et q, premiers entre eux, tels que $x = p-q$, $z = p+q$ et $y^2 = 4pq$ et p et q sont des carrés parfaits.

3. En déduire l'ensemble des éléments de E.

4. Donner tous les triplets de E tels que $z \le 18$.

29 On considère les dix caractères A, B, C, D, E, F, G, H, I et J auxquels on associe dans l'ordre les entiers de 1 à 10.
On note $\Omega = \{1, 2, 3, ..., 10\}$. On appelle message tout mot ayant un sens ou non formé avec ces dix caractères.
Soit a un entier compris entre 1 et 10. On désigne par f l'application qui à tout élément i de Ω associe le reste de a^i modulo 11.

1. On suppose que a = 5.
a. Coder à l'aide de f le message « BAC » en utilisant la grille de chiffrement ci-dessous

Message	B	A	C
i	2	1	3
$f(i)$	3		
Code	C		

b. Coder à l'aide de f le message « FADE ».
Peut-on déchiffrer avec certitude le message codé ?
2. On suppose que a = 2.
Donner la grille de chiffrement de f.
Peut-on déchiffrer avec certitude un message codé?
3. On se propose de déterminer les valeurs possibles de l'entier a pour que l'application f permette de chiffrer et de déchiffrer avec certitude tous les messages.
a. Soit i et i' deux entiers compris entre 1 et 9 tels que $i < i'$. Montrer que
$a^i \equiv a^{i'} \pmod{11}$ équivaut à $a^{i'-i} \equiv 1 \pmod{11}$.
b. En déduire que f permet de chiffrer et de déchiffrer avec certitude tous les messages, si et seulement si, a^i n'est pas congru à 1 modulo 11 pour tout $i \in \{1, 2, 3, ..., 9\}$.
c. On suppose que k est le plus petit entier de Ω tel que $a^k \equiv 1 \pmod{11}$. Montrer que k est un diviseur de 10.
d. Conclure.

30 On considère la suite de Fibonacci $(F_n)_{n\geq 0}$ définie par $F_0 = 0$; $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$, $n \geq 0$.
1. Calculer les termes de cette suite jusqu'à F_{10}.
2. Montrer que pour tout entier non nul n,
$F_{n+1} F_{n-1} - F_n^2 = (-1)^n$.
3. En déduire que pour tout entier non nul n, $F_n \wedge F_{n+1} = 1$.
4. Soit n un entier non nul. Montrer par récurrence sur l'entier m que $F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$.
5. En déduire que $F_m \wedge F_n = F_m \wedge F_{m+n}$.

31 Pour tout entier naturel n, on note $\varphi(n)$ le nombre d'entier naturels inférieurs à n et premiers avec n.
On pose $\varphi(1) = 1$.
1. Vérifier que $\varphi(7) = 6$ et $\varphi(8) = 4$.
2. Montrer que $\varphi(n) \leq n - 1$.
Soit k un entier naturel non nul, p et q deux nombres premiers et a un entier non divisible par p et q.
3. a. Montrer que $\varphi(p) = p - 1$.
b. Montrer que $a^{\varphi(p)} \equiv 1 \pmod{p}$.
4. a. Montrer que $\varphi(pq) = \varphi(p)\varphi(q)$.
b. Montrer que $a^{\varphi(pq)} \equiv 1 \pmod{pq}$.
c. En déduire les congruences ci-dessous
$10^{1536} \equiv 1 \pmod{1649}$;
$10430^{10200} \equiv 1 \pmod{10403}$.
5. a. Montrer que $\varphi(p^k) = p^k - p^{k-1}$.
b. Déterminer $\varphi(125)$, $\varphi(256)$ et $\varphi(1331)$.
6. a. Montrer que $(1+up)^{p^{k-1}} \equiv 1 \pmod{p^k}$
(On pourra utiliser que tout entier non nul n divise C_n^j, $j \neq 0$ et $j \neq n$).
b. Montrer que $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$.
En déduire les congruences ci-dessous
$17^{100} \equiv 1 \pmod{125}$; $17^{128} \equiv 1 \pmod{256}$.

CH 8 IDENTITE DE BEZOUT

Q.C.M :

1. L'entier 5 est un inverse modulo 6 de 5 en effet $5x5=25=6x4+1\equiv 1(6)$
2. Si p est un entier premier alors $p\wedge p^2=p$
3. L'ensemble des solutions entières de l'équation $11x-5y=1$ est :
   $\{(1+5k\ ;2+11k), k\in\mathbb{Z}\}$
4. L'ensemble des solutions entières de l'équation $13x-17y=0$ est :
   $\{(17k\ ;13k), k\in\mathbb{Z}\}$

VRAI-FAUX :

1. $n \equiv 0\ (143)$ ssi $n\equiv 0(13)$ et $n\equiv 0(11)$ (VRAI)

   Justification :($\Rightarrow$) si $n \equiv 0\ (143)$ alors $n=k.143=k.11.13 \Rightarrow n\equiv 0(13)$
   et $\Rightarrow n\equiv 0(11)$
   ($\Leftarrow$)Si $n\equiv 0(13)$ et $n\equiv 0(11)$ Alors $n\equiv 0(11x13)$ car $11\wedge 13=1$
   Alors $n\equiv 0(143)$

2. $-3a\ \hat{}\ 3b = 3(a\hat{}b)$ (VRAI)
   Justification: $-3a\hat{}3b=3(-a\hat{}b)=3(a\hat{}b)$

$k.a\hat{}k.b=\lvert k\rvert(a\hat{}b)$
$a\wedge b=\lvert a\rvert\wedge\lvert b\rvert$

3. $25x-80y=3$ admet des solutions entières (FAUX)
   Justification: on a $25\hat{}80= 5$ et 5 ne divise pas 3

4. Tout entier admet un inverse modulo 14 (FAUX)
   Justification: 2 n'admet pas un inverse modulo 14

5. Pour tout entier $n \geq 2$; $n-1$ est son propre inverse modulo n (VRAI)
   Justification : $n-1\equiv -1(n) \Rightarrow (n-1)^2\equiv(-1)^2(n)\Rightarrow(n-1).(n-1)\equiv 1(n)$

CH 8 IDENTITE DE BEZOUT

EX 1 page 175 :

558 ^ (-1235) = 1 Algorithme d'Euclide(pour le calcul du pgcd)

r	1 235	558	119	82	37	8	5	3	2	1	0
q	-	-	2	4	1	2	4	1	1	1	2

1 est le dernier reste non nul

924 ^ 990 = 66

(-999) ^ (888) = 111

1890 ^ (-5250) = 210

EX 2 page 175 :

558 ^ (-1235) = 1 ⇒ 558 v (-1235) = 558 x 1235 =726 180

51 ^ (- 255) = 51 ⇒ 51 v (-255) = $\frac{51\times 255}{51} = 255$

(2 n +1) ^ n = 1 ⇒(2n +1) v n = | n.(2n +1) |

EX 3 page 175 :

$$\left.\begin{array}{l} 180 = 36\times 5 \\ a \wedge 180 = 36 \end{array}\right\} \Rightarrow a = 36.k \text{ avec } k \text{ n'est pas un multiple de } 5$$

$$|a| < 360 \Rightarrow k \in \{\pm 1;\pm 2;\pm 3;\pm 4;\pm 6;\pm 7;\pm 8;\pm 9\}$$

$$a \in \{\pm 36;\pm 72;\pm 108;\pm 144;\pm 216;\pm 252;\pm 288;\pm 324\}$$

EX 4 page 175 :

a^b=19 ⇒ a =k.19 et b=k'.19

a.b=2166 = 2x3x19x19 ⟩ $k \in \{\pm 1;\pm 2;\pm 3;\pm 6\}$

Donc (a ;b) $\in \left\{\begin{array}{l}(19;114),(114;19),(38;57)(57;38), \\ (-19;-114),(-114;-19),(-38;-57),(-57:-38)\end{array}\right\}$

EX 5 page 175 : (Raisonnement par l'absurde)

Supposons qu'il existe un couple (a ;b) tels que : a^b=19 et a^2-b^2 =490.

a^b=19 $\Rightarrow \left.\begin{array}{l} 19|a \\ 19|b \end{array}\right\} \Rightarrow 19|a-b \Rightarrow 19|(a-b).(a+b) \Rightarrow 19|a^2-b^2$

19|490 absurde

CH 8 IDENTITE DE BEZOUT

EX 6 :

1. $2^5 = 32 = 11x3 - 1 \Rightarrow 2^5 \equiv -1(11)$

   $2^5 = 32 = 31x1+1 \Rightarrow 2^5 \equiv 1(31)$

2. **On a $2^5 \equiv -1(11) \Rightarrow (2^5)^{68} \equiv (-1)^{68}(11) \Rightarrow 2^{340} \equiv 1(11)$**

   On a $2^5 \equiv 1(31) \Rightarrow (2^5)^{68} \equiv 1^{68}(31) \Rightarrow 2^{340} \equiv 1(31)$

3. $\left.\begin{array}{l} on\ a\ 2^{340} \equiv 1(31) \Rightarrow 31 divise\ 2^{340}-1 \\ on\ a\ 2^{340} \equiv 1(11) \Rightarrow 11\ divise\ 2^{340}-1 \\ \qquad\qquad et\ comme\ 31 \wedge 11 = 1 \end{array}\right\} \Rightarrow 11 \times 31 = 341 divise 2^{340} - 1$

EX 7 :

1. a^561=1 $\Rightarrow a \wedge (3.11.17) = 1 \Rightarrow \left.\begin{array}{l} a\ n'est\ pas\ un\ multiple\ de\ 3 \\ et\ comme\ 3\ nombre\ premier \end{array}\right\} \Rightarrow a \wedge 3 = 1$

   de même on montre que a^11=1 et a^17=1

2. a/

   $\left.\begin{array}{l} 3\ un\ nombre\ premier \\ a\ n'est\ pas\ un\ multiple\ de\ 3 \end{array}\right\} \overset{fermat}{\Rightarrow} a^{3-1} \equiv 1(3) \Rightarrow a^2 - 1 \equiv 0(3) \Rightarrow 3\ divise\ a^2 - 1$

   b/ de même que a/

   c/ de même que a/

3. a/ On a $a^2 \equiv 1(3) \Rightarrow (a^2)^{280} \equiv 1^{280}(3) \Rightarrow a^{560} \equiv 1(3)$

   On a $a^{10} \equiv 1(11) \Rightarrow (a^{10})^{56} \equiv 1^{56}(11) \Rightarrow a^{560} \equiv 1(11)$

   On a $a^{16} \equiv 1(17) \Rightarrow (a^{16})^{35} \equiv 1^{35}(17) \Rightarrow a^{560} \equiv 1(17)$

   b/

   $\left.\begin{array}{l} a^{560} \equiv 1(17) \Rightarrow 17\ divise\ a^{560} - 1 \\ a^{560} \equiv 1(11) \Rightarrow 11\ divise\ a^{560} - 1 \\ \qquad\qquad et\ comme\ 11 \wedge 17 = 1 \end{array}\right\} \Rightarrow 11 \times 17 divise\ a^{560} - 1 \Rightarrow 187 divise\ a^{560} - 1$

   $\left.\begin{array}{l} on\ a\quad a^{560} \equiv 1(3) \Rightarrow 3\ divise\ a^{560} - 1 \\ \qquad\qquad et\ on\ a\ 187 divise\ a^{560} - 1 \\ \qquad\qquad\qquad 3 \wedge 187 = 1 \end{array}\right\} \Rightarrow 3 \times 187 divise\ a^{560} - 1 \Rightarrow 561\ divise\ a^{560} - 1$

CH 8 IDENTITE DE BEZOUT

EX 8 :

1. $\left.\begin{matrix} n|4a+5b \\ n|5a+2b \end{matrix}\right\} \Rightarrow n|5.(5a+2b)-2(4a+5b) \Rightarrow n|17a$

$\left.\begin{matrix} n|4a+5b \\ n|5a+2b \end{matrix}\right\} \Rightarrow n|5.(4a+5b)-4.(5a+2b) \Rightarrow n|17b$

2. Soit h= (4a+5b)∧(5a+2b).

On a d=a∧b $\Rightarrow \left.\begin{matrix} d|a \\ d|b \end{matrix}\right\} \Rightarrow \left.\begin{matrix} d|4a+5b \\ d|5a+2b \end{matrix}\right\} \Rightarrow d|h \Rightarrow h = k.d$

h=(4a+5b)∧(5a+2b) $\Rightarrow \left.\begin{matrix} h|4a+5b \\ h|5a+2b \end{matrix}\right\} \overset{d'après\,1}{\Rightarrow} \left.\begin{matrix} h|17a \\ h|17b \end{matrix}\right\} \Rightarrow h|17a \wedge 17b \Rightarrow h|17(a \wedge b) \Rightarrow k.d|17.d \Rightarrow k|17$

$\Rightarrow$ k=1 ou k=17

$\Rightarrow$ h=d ou h=17d

EX 9 :

1. Si d divise a et b alors d divise toute combinaison linéaire de a et b et en particulier d divise a+bn et a+b(n-1)

2. Si d divise a+bn et a+b(n-1) Alors d divise a+bn-(a+b(n-1))= b donc d divise b et par suite d divise bn

d divise a+bn et d divise bn Alors d divise a

3. Soient d = a^b et d' = (

* d =a^b Alors d divise a et b Alors (d'après 1/) d divise a+bn et a+b(n-1)
  Donc d divise d'

* d' =(a+bn)^(a+b(n-1)) Alors d' divise a+bn et a+b(n-1)
  Alors (d'après 2.) d' divise a et d' divise b donc d' divise d

On a d divise d' et d' divise d Donc d'=d

Conclusion : $\boxed{(a+bn) \wedge (a+b)(n-1)) = a \wedge b}$

CH 8 IDENTITE DE BEZOUT

EX 10 : (L'algorithme d'Euclide-Bézout)
C'est ;d'après M Achour Abdennebi* ;le plus important des algorithmes de l'Arithmétique.
Etant donné deux entiers a et b(b>a>0) ;le tableau ci-dessous
Suggère ce qu'il faut faire.

	1	2	3	...	i	i+1	...	n	
r	b	a	R_3=le reste de b/a	...	r_i	R_{i+1}= le reste de r_{i-1}/r_i		r_n	0
q	-	-	Q_3=le quotient de b/a	...	q_i	Q_{i-1}= le quotient de r_{i-1}/ri	...	q_n	
x	$X_1=0$	$X_2=1$	$X_3=q_3.x_2+x_1$	...	x_i	$X_{i+1}=q_{i+1}.x_i+x_{i-1}$	...	x_n	
y	$Y_1=1$	$Y_2=0$	$Y_3=q_3.y_2+y_1$	...	y_i	$Y_{i+1}=q_{i+1}.y_i+y_{i-1}$	...	y_n	

* r_n le dernier reste non nul est le pgcd de a et b .

* $a.xn - b.yn = \pm r_n$

Appliqué au cas a =2015 et b = 2007 , cet algorithme donne

r	2015	2007	8	7	1	0
q	-	-	1	250	1	7
x	0	1	1.1+0=1	250 .1+1=251	1.251+1=252	-
y	1	0	1.0+1=1	250.1+0=250	1.250+1=251	-

. Le dernier reste non nul est 1 Donc 2015^2007 = 1.
. L'identité de Bézout s'écrit : 2015x251-2007x252 =1 Donc a = (-252) et b=251

EX 11 :
Appliquons encore une fois l'algorithme d'Euclide-Bézout au cas a=323 et b=391

r	391	323	68	51	17	0
q	-	-	1	4	1	3
x	0	1	1	5	6	-
y	1	0	1	4	5	

1. Le dernier reste non nul est 17 Donc 391∧323=17
2. L'identité de Bézout s'écrit : 391X5-323X6=17 Donc a=5 et b=-6
3. En déduire une solution de 391a-323b=306
   On remarque que 306= 17x18 Donc a=5x18 et b= (-6)x18

CH8 IDENTITE DE BEZOUT

EX12 :

1. L'algorithme d'Euclide Bézout donne

r	97	11	9	2	1	0
q	-	-	8	1	4	2
x	0	1	8	9	44	-
y	1	0	1	1	5	-

L'identité de Bézout s'ecrit : 97x5-11x44 = 1donc (5,-44) est une solution particulière

$$97x+11y=1 \Leftrightarrow 97x+11y=97.5+11.(-44) \Leftrightarrow 97.(x-5)=11.(-44-y) \Rightarrow \left.\begin{matrix} 11|97(x-5) \\ or\ \ 11\wedge 97=1 \end{matrix}\right) \Rightarrow 11|x-5$$

$$\Rightarrow x=11k+5$$

$97x+11y=1 \Rightarrow 11y=1-97x \Rightarrow 11y=1-97.(11k+5) \Rightarrow y=-97k-44$

Réciproquement si (x,y)=(11k+5,-97k-44) Alors 97x+11y=97(11k+5)+11(-97k-44)

Conclusion : $S_{\mathbb{Z}x\mathbb{Z}}=\{(11k+5,-97k-44),\ k\in\mathbb{Z}\}$

2.

a/ L'algorithme d'Euclide Bézout donne 97x27 -77x34=1

En multipliant par 7 on obtient : $97.(27x7)-77.(34x7)=7 \Leftrightarrow 97.189+77.(-238)=7$
donc une solution particulière de (E) est (189 ;-238)

b/ On a 97.189 -77.238=7 Donc $97x+77y=7 \Leftrightarrow 97x+77y=97.189-77.238$

$$\Leftrightarrow 97(x-189) = -77(y+238)$$

$$\Rightarrow \left.\begin{matrix} 77|97.(x-189) \\ or\ \ 77\wedge 97=1 \end{matrix}\right) \Rightarrow 77|x-189 \Rightarrow x=77k+189$$

$97x+77y=7 \Rightarrow 77y = 7-97x \Rightarrow 77y=7-97(77k+189) \Rightarrow y= -238-97k$

Réciproquement si (x,y)=(77k+189 ;-97k-238)
Alors 97x+77y=97.(77k+189)+77.(-97k-238)=7

CI : $S_{\mathbb{Z}x\mathbb{Z}}=\{(77k+189\ ;-97k-238)\}$

CH 8 Identité de Bézout

EX 13 :

1. a/ * Pour n=1 $u^n = u^1 = u = 2+\sqrt{3} = a_1 + b_1\sqrt{3}$ avec $a_1 = 2$ et $b_1 = 1$ deux entiers naturels

Donc la propriété est vrai à l'ordre initial

* Soit $n \in \mathbb{N}^*$ Supposons que $u^n = a_n + b_n\sqrt{3}$ avec a_n et b_n deux entiers

et montrons que $u^{n+1} = a_{n+1} + b_{n+1}\sqrt{3}$ avec a_{n+1} et b_{n+1} deux entiers

On a $u^n = a_n + b_n\sqrt{3} \Rightarrow u^{n+1} = u.u^n = (2+\sqrt{3})(a_n + b_n\sqrt{3}) = (2a_n+3b_n)+(2b_n+a_n)\sqrt{3}$

$= a_{n+1} + b_{n+1}\sqrt{3}$

Comme a_n et b_n sont deux entiers naturelles alors $a_{n+1} = 2a_n+3b_n$ et $b_{n+1} = 2b_n+a_n$ sont deux entiers naturelles

Cl : pour tout $n \in \mathbb{N}^*$ $u^n = a_n + b_n\sqrt{3}$ avec a_n et b_n deux entiers naturelles

b/ $a_{n+1} = 2a_n+3b_n$ et $b_{n+1} = 2b_n+a_n$

2. a/ (Par recurrence)

* Pour n=1 $a_n^2 - 3b_n^2 = a_1^2 - 3b_1^2 = 2^2 - 3\times 1^2 = 1$

* Soit $n \in \mathbb{N}^*$ Supposons que $a_n^2 - 3b_n^2 = 1$ *et montrons que* $a_{n+1}^2 - 3b_{n+1}^2 = 1$

$$a_{n+1}^2 - 3b_{n+1}^2 = (2a_n+3b_n)^2 - 3(a_n+2b_n)^2$$
$$= 4a_n^2 - 3a_n^2 + 9b_n^2 - 12b_n^2 + 12a_nb_n - 12a_nb_n$$
$$= a_n^2 - 3b_n^2 = 1$$

$$a_nb_{n+1} - a_{n+1}b_n = a_n.(a_n+2b_n) - (2a_n+3b_n)b_n$$
$$= a_n^2 + 2a_nb_n - 2a_nb_n - 3b_n^2 = a_n^2 - 3b_n^2 = 1$$

b/ On a $\forall n \geq 1$ $\left.\begin{array}{l} a_n \text{ et } b_n \text{ deux entiers naturelles} \\ a_nb_{n+1} - a_{n+1}b_n = 1 \end{array}\right\} \overset{\text{bezout}}{\Rightarrow}$ $a_n \wedge b_n = 1 = a_n \wedge a_{n+1} = b_{n+1} \wedge b_n$

EX 14:

a/ 7^14=7 ne divise pas 5 donc l'équation 7x-14y =5 n'admet pas de solutions

b/ $5x-10y=10 \Leftrightarrow x-2y=2 \Leftrightarrow x=2+2y$ Donc $S_{\mathbb{Z}\times\mathbb{Z}} = \{(2+2k,k)\ k \in \mathbb{Z}\}$

c/ 29^58=29 ne divise pas 3 donc l'équation 29x+58y=3 n'admet pas de solutions

CH8 IDENTITE DE BEZOUT

EX 15 :

1. $(4x-3y-5)(4x+3y-1)=0 \Leftrightarrow 4x-3y=5$ ou $4x+3y=1$

(1 ;-1) est une solution particulière trivial de l'équation $4x+3y=1$ alors un travail analogue à l'exercice 12 permet de conclure que les solutions de l'éq $4x+3y=1$ sont les couples $(1+3k ;-1-4k)$ k entier

(5 ;5) est une solution particulière trivial de l'équation $4x-3y=5$ alors un travail analogue à l'exercice 12 permet de conclure que les solutions de l'éq $4x-3y=5$ sont les couples $(5+3k ;5+4k)$ k entier .

Conclusion :

$$S_{\mathbb{Z}\times\mathbb{Z}}=\{(1+3k ;-1-4k) ;(5+3k ;5+4k)\ k\in\mathbb{Z}\ \}$$

2. $x^2-9y^2=2 \Leftrightarrow (x-3y).(x+3y)=2 \Leftrightarrow$ $\begin{cases}x-3y=2\\x+3y=1\end{cases}$ *ou* $\begin{cases}x-3y=1\\x+3y=2\end{cases}$ *ou* $\begin{cases}x-3y=-2\\x+3y=-1\end{cases}$ *ou* $\begin{cases}x-3y=-1\\x+3y=-2\end{cases}$

chacun de ces 4 systèmes n'a pas de solution dans $\mathbb{Z}\times\mathbb{Z}$ (en effet on obtient $2x=3$ ou $2x=-3$) donc l'équation $x^2-9y^2=2$ n'a pas de solution dans $\mathbb{Z}\times\mathbb{Z}$

EX 16 :

1. (-3,-5) est une solution particulière trivial de l'équation $13x-8y=1$ alors un travail analogue à l'exercice 12 permet de conclure que les solutions de l'éq $13x-8y=1$ sont les couples $(-3+8k ;-5+13k)$ k entier.

2. Si (x,y,z) solution de S Alors en faisant la somme on obtient : $13x-8y=1$ donc (x,y) est une solution de (E).

$5x+y-2z=1 \Leftrightarrow 2z=5x+y-1=5(8k-3)+13k-5-1=53k-21$ un nombre pair

donc k entier impair

donc k = 2p+1 p entier

Cl : $S_{\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}}=\left\{\left(8k-3,13k-5,\frac{53k-21}{2}\right),k=2p+1\quad p\in\mathbb{Z}\right\}$

$=\{(16p+5,26p+8,53p+16).\ p\in\mathbb{Z}\}$

CH8 IDENTITE DE BEZOUT

EX 17 :

1. On remarque que (5,4) est une solution particulière triviale de
   L'équation 9u-11v=1 (si non l'algorithme d'Euclide-Bezout permet d'en trouver)

2. $$\left.\begin{array}{l} x\equiv a(9) \\ x\equiv b(11) \end{array}\right\}\Rightarrow \left.\begin{array}{l} x=9k+a \\ x=11k'+b \end{array}\right\}\Rightarrow \left.\begin{array}{l} 44x=396k+44a \\ 45x=495k'+45b \end{array}\right\}\Rightarrow x=(495k'-396k)+(45b-44a)$$
   $$\Rightarrow \quad x=99.(5k'-4k)+(45b-44a)$$
   $$\Rightarrow \quad x\equiv(45b-44a)\,(99)^{\backslash}$$

3. $\begin{cases} x\equiv 6(9) \\ x\equiv 8(11) \end{cases}\Rightarrow$ (d'apres 2.) x≡(45x8-44x6)(99)⇒x≡96(99)⇒x=k.99+96

   Réciproquement : si x=k.99+96⇒x-6=9.(k.11+10)⇒x≡6(9)

   ⇓

   x-8=k.99+88⇒x-8=11.(k.9+8)⇒x≡8(11)

EX 18 :

1. a/ 5x7=35=17.2+1≡1(17) donc 7 est une solution particulière

   b/ 5x≡1(17) ⇔5x≡5.7(17)⇔5(x-7)≡0(17)$\Rightarrow \left.\begin{array}{l} 17\mid 5(x-7) \\ or\ 17\wedge 5=1 \end{array}\right\}\Rightarrow 17\mid x-7\Rightarrow x=17k+7$

   Cl : $S_{\mathbb{Z}}=\{17.k+7\ ;\ k\in\mathbb{Z}\}$

   c/ On a 345=17x20+5⇒345≡5(17) Donc

   345x≡1(17)⇔5x≡1(17) Alors d'après b/ $S_{\mathbb{Z}}=\{17.k+7\ ;\ k\in\mathbb{Z}\}$

2. a/ 5x14=70=17x4+2 Donc 14 est une solution particulière de 5x≡2(17)

   Donc 5x≡2(17)⇔5x≡5.14(17)⇔5(x-14)≡0(17)$\left.\begin{array}{l} 17\mid 5(x-14) \\ or\ 17\wedge 5=1 \end{array}\right\}\Rightarrow 17\mid x-14\Rightarrow x=17k+14$

   Cl : $S_{\mathbb{Z}}=\{17.k+14\ ;\ k\in\mathbb{Z}\}$

   b/ On a 430=17x25+5⇒430≡5(17) Donc

   430x≡2(17) ⇔5x≡2(17) Alors d'après a/ $S_{\mathbb{Z}}=\{17.k+14\ ;\ k\in\mathbb{Z}\}$

CH8 IDENTITE DE BEZOUT

EX 19

1. $17x\equiv 1(33)$ On remarque que 2 est une solution particulière donc

$$17x\equiv 1(33) \Leftrightarrow 17x\equiv 17.2(33)\Leftrightarrow 17.(x-2)\equiv 0(33)\Rightarrow \left.\begin{matrix}33\mid 17(x-2)\\ or\ 33\wedge 17=1\end{matrix}\right)\Rightarrow 33\mid x-2\Rightarrow x=33k+2$$

Cl : $S_{\mathbb{Z}}=\{33k+2, k\in\mathbb{Z}\}$

2. Ona $17x2\equiv 1(33)\Rightarrow 17x2x(-9)\equiv -9(33)$ donc $2x(-9)=-18\equiv 15(33)$ est une solution particulière Donc $17x\equiv -9(33) \Leftrightarrow 17x\equiv 17.15(33)\Leftrightarrow 17(x-15)\equiv 0(33) \Rightarrow$

33 divise 17(x-15) et comme $33\wedge 17=1$ Donc 33divise $x-15\Rightarrow x=33k+15$

Cl : $S_{\mathbb{Z}}=\{33k+15, k\in\mathbb{Z}\}$

EX 20

$12x\equiv 30y(15) \Leftrightarrow 12x\equiv 0(15)\Leftrightarrow 12x=15k\Leftrightarrow 4x=5k\Rightarrow 5$ divise 4x et comme $5\wedge 4=1\Rightarrow 5$ divise x

Donc x est un multiple de 5 et y est quelconque

Donc l'ensemble des couples (x,y) $/12x\equiv 30y(15)$ est $\{(5k,y) ; k\in\mathbb{Z} \text{ et } y\in\mathbb{Z}\}$

EX 21

$11x\equiv 99y(77)\Leftrightarrow 11x= k.77+99y\Leftrightarrow x=k.7+9y$

Donc l'ensemble des couples (x,y) $/11x\equiv 99y(77)$ est $\{(7k+9y,y) ; k\in\mathbb{Z} \text{ et } y\in\mathbb{Z}\}$

EX 22

1. Soit $d=a\wedge b \Rightarrow d \mid 2b-3a=7\Rightarrow d=1$ ou d=7 Donc les valeurs possibles de $a\wedge b$ sont 1 et 7
2. a/ $3a-2b= 3(2n-3)-2(3n-1)= -7$ Donc pour tout n le couple(a,b) est une solution de (E).

b/ (E) : $3x-2y=-7\Leftrightarrow 3x-2y=3a-2b\Leftrightarrow 3(x-a)=2(y-b)$

$\Rightarrow 3 \mid 2(y-b)$ et comme $3\wedge 2=1$ Donc $3 \mid y-b\Rightarrow y= 3k+b=3k+3n-1=3(k+n)-1=3h-1$

Remplacons y par 3h-1 dans (E) on obtient : $3x=2(3h-1)-7\Rightarrow x=2h-3$

Cl : $S_{\mathbb{Z}x\mathbb{Z}}=\{(2h-3,3h-1) ; h\in\mathbb{Z}\}$

3. $a\wedge b=7\Rightarrow a\equiv 0(7)$ et $b\equiv 0(7)\Rightarrow a\equiv b(7)\Rightarrow 3n-1\equiv 2n-3(7)\Rightarrow n\equiv -2(7)\Rightarrow n\equiv 5(7)$

Réciproquement si $n\equiv 5(7) \Rightarrow n=7k+5 \Rightarrow a=2(7k+5)-3=14k+7=7(2k+1)\Rightarrow 7 \mid a$

$\Downarrow$

$b=3(7k+5)-1=21k-14=7(3k-2)\Rightarrow 7 \mid b$

On a donc 7 | a et 7 | b et comme les valeurs possibles de $a\wedge b$ sont 1 et 7 donc

Cl : $\boxed{a\wedge b=7 \quad ssi \quad n=5+7k \ ; k\in\mathbb{Z}}$

CH 8 IDENTITE DE BEZOUT

EX23 :

1. $a\wedge n=1\Rightarrow a\wedge pqu=1\Rightarrow a\wedge p=1$; $a\wedge q=1$ et $a\wedge u=1$

$a\wedge p=1$ et p premier alors d'apré th de Fermat $a^{p-1}\equiv 1(p)$

$a\wedge q=1$ et q premier alors d'apré th de Fermat $a^{q-1}\equiv 1(q)$

$a\wedge u=1$ et u premier alors d'apré th de Fermat $a^{u-1}\equiv 1(u)$

On a p-1 divise n-1 donc $n-1=k.(p-1)\Rightarrow a^{n-1}=(a^{p-1})^k\equiv 1^k\ (p)\Rightarrow a^{n-1}\equiv 1(p)$

On a q-1 divise n-1 donc $n-1=k.(q-1)\Rightarrow a^{n-1}=(a^{q-1})^k\equiv 1^k\ (q)\Rightarrow a^{n-1}\equiv 1(q)$

On a u-1 divise n-1 donc $n-1=k.(u-1)\Rightarrow a^{n-1}=(a^{u-1})^k\equiv 1^k\ (u)\Rightarrow a^{n-1}\equiv 1(u)$

2. On a $a^{n-1}-1\equiv 0(p)$; $a^{n-1}-1\equiv 0(q)$ et $p\wedge q=1$ Alors $a^{n-1}-1\equiv 0(pq)$

On a $a^{n-1}-1\equiv 0(pq)$; $a^{n-1}-1\equiv 0(u)$ et $pq\wedge n=1$ Alors $a^{n-1}-1\equiv 0(pqu)$ donc $a^{n-1}-1\equiv 0(n)$

3. $561=3x11x17$ On pose n=561 ; p=3 ;q=11 ; u=17 et a=224

Alors d'après les questions 1. et 2. on peut conclure que $224^{560}\equiv 1(561)$

4. $1729=7x13x19$ on pose n=1729 ; p=7 ;q=13 ; u=19 et a=561

Alors d'après les questions 1. et 2. on peut conclure que $561^{1728}\equiv 1(1729)$

EX 24 :

1.

a/ On a $(a+b)\wedge ab=p\Rightarrow$ p divise ab et p divise a+b

Supposons que p ne divise pas a ; comme p est premier alors $p\wedge a=1$

On a $p \mid ab$ et $p\wedge a=1$ donc p divise b et comme $p \mid a+b$ Alors $p \mid a$ Absurde

Donc p divise a et comme p divise a+b Alors p divise aussi b

donc p est un diviseur commun de a et b.

b/ Soit $d=a\wedge b$

On a p est un diviseur commun de a et b Donc p divise d

$d=a\wedge b\Rightarrow$ d divise a et b $\Rightarrow$ d divise a+b et ab $\Rightarrow$ d divise p

On a donc d divise p et p divise d Donc p=d Donc $p=a\wedge b$

2. a/ $\begin{cases} a\wedge b=5 \\ a\vee b=170 \end{cases}\Rightarrow$ a et b sont des multiples de 5 et axb=5x170=5x(5x2x17)

Et comme a≤b Alors a=5 et b=5x2x17=170 ou a=5x2 et b=5x17=85

b/ 5 étant un nombre premier alors d'apres 1. (a+b)^a.b=a^b Alors

$$\begin{cases} (a+b)\wedge ab=5 \\ a\vee b=170 \end{cases}\Leftrightarrow\begin{cases} a\wedge b=5 \\ a\vee b=170 \end{cases}$$

Alors a=5 et b=170 ou a=10 et b=85 (d'après 2. a/)

CH 8 Identité de Bézout

EX 25 :

1. $363 \wedge 484 = 121$ (Algorithme d'Euclide)

   On a $363 \wedge 484 = 121$ et $484 - 363 = 121$ Donc $(363,484) \in S$

2. $n \wedge n+1 = 1 = n+1-n$ Donc $(n ; n+1) \in S$

3.

   a/ ($\Rightarrow$)

   s'il existe $k \in IN^*$ / $x = k(y-x)$ et $y = (k+1)(y-x)$ $x < y$ Alors

   $x \wedge y = k(y-x) \wedge (k+1)(y-x) = |y-x| \, (k \wedge k+1) = (y-x).1 = y-x$ Donc $(x,y) \in S$

   ($\Leftarrow$) si $(x;y) \in S$ Alors $x < y$ et $x \wedge y = y-x \Rightarrow (y-x) \mid x$ et $(y-x) \mid y$

   $\Rightarrow x = k(y-x)$ et $y = k'(y-x)$

   $\Rightarrow y-x = (k'-k)(y-x) \Rightarrow k'-k = 1 \Rightarrow k' = k+1$

   Donc $x = k.(y-x)$ et $y = (k+1)(y-x)$

Cl : $(x;y) \in S$ ssi il existe $k \in IN^*$ / $x = k(y-x)$ et $y = (k+1)(y-x)$ $x < y$

b/ $(x;y) \in S$ donc il existe $k \in IN^*$ / $x = k(y-x)$ et $y = (k+1)(y-x)$

Donc $x \vee y = \dfrac{x.y}{x \wedge y} = \dfrac{k(y-x).(k+1)(y-x)}{y-x} = k(k+1)(y-x)$

4. a/ $D_{228} = \{1 ; 2 ; 3 ; 4 ; 6 ; 12 ; 19 ; 38 ; 57 ; 76 ; 114 ; 228\}$

   b/ $(x;y) \in S$ et $x \vee y = 228 \Rightarrow 228 = k.(k+1)(y-x)$ Donc k ; k+1 et y-x sont des diviseurs de 228

Donc les valeurs possibles de k sont 1 ; 2 ou 3

$k=1 \Rightarrow y-x = 114 \Rightarrow x = k.(y-x) = 114$ et $y = (k+1)(y-x) = 228$

$k=2 \Rightarrow y-x = 38 \Rightarrow x = 2 \times 38 = 76$ et $y = 3 \times 38 = 114$

$k=3 \Rightarrow y-x = 19 \Rightarrow x = 3 \times 19 = 57$ et $y = 4 \times 19 = 76$

Conclusion : L'ensemble des couples (x,y) de S tel que $x \vee y = 228$ est $\{(114,128) ; (76,114) ; (57,76)\}$

CH8 IDENTITE DE BEZOUT

EX 26 :

1. a/ M(z) est invariant par f ssi z'=z en posant z=x+iy

$$\text{ssi } \frac{3+4i}{5}(x-iy)+\frac{1-2i}{5}=x+iy$$

ssi (3+4i)(x-iy)+1-2i=5(x+iy)

ssi 1+3x+4y+i(4x-3y-2)=5x+i5y

$$\text{ssi } \begin{cases}1+3x+4y=5x\\4x-3y-2=5y\end{cases}\Leftrightarrow\begin{cases}2x-4y-1=0\\4x-8y-2=0\end{cases}\Leftrightarrow 2x-4y-1=0$$

Conclusion : L'ensemble des points invariants par f est la droite Δ d'équation

Δ : 2x-4y-1=0

b/ f est une similitude indirecte de rapport k= $\left|\frac{3+4i}{5}\right|=1$ donc f est un antidéplacement ayants des points invariants donc f est une symétrie axiale d'axe la droit Δ :2x-4y-1=0

2. a/ z' réel ⇔ Im(z')=0⇔4x-3y-2=0 Donc D est la droite d'éq :4x-3y-2=0

b/ 4x-3y=2 (2 ;2) est une solution particulière triviale

un travail analogue à l'ex 12 permet de trouver $S_{\mathbb{Z}\times\mathbb{Z}}=\{(3k+2\ ;4k+2)\ ;k\in\mathbb{Z}\}$

c/ Les poits de D dont les coordonnées sont des entiers sont :M=(3k+2 ;4k+2) ;k∈ℤ

1. z=1+iy ⇒ $z'=\frac{3+4i}{5}(1-iy)+\frac{1-2i}{5}=\frac{4+4y+i(2-3y)}{5}$

réel(z') entier $\Leftrightarrow\frac{4+4y}{5}=k\Leftrightarrow 4(1+y)=5k\Leftrightarrow\left.\begin{matrix}5|4(1+y)\\or\ 5\wedge 4=1\end{matrix}\right)\Rightarrow 5|1+y$ ⇒y=5k-1

y=5k-1 ⇒ $Im(z')=\frac{2-3(5k-1)}{5}=\frac{5-15k}{5}=1-3k$ ⇒ Im(z') est un entier

Cl : Réel(z') et Im(z') sont entiers ssi y=5k-1 ; k∈ℤ

EX 27

1. $(a^2+ab-b^2)^2=1$ ⇒ $a^2+ab-b^2=1$ ou $a^2+ab-b^2=-1$

⇒ a(a+b)-b.b=1 ou a(a+b)-b.b=-1 Alors d'aprés th de Bézout a et b sont premiers entre eux

2. Si x=y alors (E) ⇔ $(xy)^2=1\Leftrightarrow x^4=1\Leftrightarrow x=1$ ou x=-1

Cl : Les solutions de (E) telles que x=y sont (1,1) et (-1,-1)

3. a/ (p,q) solution ⇒ $(p^2+pq-q^2)^2=1$

$(q^2+q(p+q)-(p+q)^2)^2=(q^2+pq+q^2-p^2-q^2-2pq)^2=(-p^2-pq+q^2)^2=(p^2+pq-q^2)^2=1$

Donc (q,p+q) est une solution de (E).

b/ On a (q,p+q) est une solution de (E) Alors d'après a/ (p+q,q+p+q) solution

Donc (p+q,p+2q) est une solution de (E)

c/ On a (1,1) solution ,en utilisant 3. a/ on obtient (1,2) ;(2, 3) ;(3,5) ;(5,8) et (8,13) solutions de (E).

EX 28 :

1. On a $(a^2-b^2)^2+(2ab)^2=(a^2+b^2)^2$ Donc $(a^2-b^2\ ;2ab\ ;a^2+b^2) \in E$.

2. a/ (x,y,z) élément de E donc $x^2+y^2=z^2$

$$x\wedge y=1 \Leftrightarrow x^2\wedge y^2=1 \Rightarrow x^2\wedge(x^2+y^2)=1\Rightarrow x^2\wedge z^2=1\Rightarrow x\wedge z=1$$

$$\Downarrow$$

$$(x^2+y^2)\wedge y^2=1\Rightarrow z^2\wedge y^2=1\Rightarrow z\wedge y=1$$

b/ Si x et y sont tout les deus paires alors 2 est un diviseur commun de x et y ce qui est absurde car pgcd(x,y)=1

c/ Les restes possibles d'un entier a modulo 4 sont :0 ;1 ;2 ;3.

Alors le tableau de congruence suivant

Reste modulo 4 de a	0	1	2	3
Reste modulo 4 de a^2	0	1	0	1

prouve que. l'équation :$a^2\equiv 2\ (4)$ ne Possède pas de solution entière

d/ Si x et y sont impairs$\Rightarrow x=2k+1$ et $y=2k'+1$

Donc $z^2=x^2+y^2=(2k+1)^2+(2k'+1)^2=4.(k^2+k'^2+k+k')+2\equiv 2(4)$ absurde

Car l'équation :$a^2\equiv 2\ (4)$ ne Possède pas de solution entière

Donc x et y ne sont pas tout les deux impairs .

d/ (x impair et y pair)$\Rightarrow$(x^2 impair et y^2 pair)$\Rightarrow x^2+y^2$ impair$\Rightarrow z^2$ impair$\Rightarrow$ zimpair

(x impair et z impair)$\Rightarrow$ z+x et z-x sont pairs.$\Rightarrow$ il existe deux entiers

Strictement positifs p et q / $z+x=2p$ et $z-x=2q$ (car x,yet $z\in IN^*$

Et $x^2+y^2=z^2\Rightarrow z>x$)

$(z+x=2p$ et $z-x=2q)\Rightarrow x=p-q$ et $z=p+q$ et $y^2=z^2-x^2=(p+q)^2-(p-q)^2=4pq$

Soit $d=p\wedge q\Rightarrow$d divise p etq$\Rightarrow$d divise p+q etp-q$\Rightarrow$d divse z et $x\Rightarrow d=1$ car $x\wedge y=1$

Donc p et q sont premiers entre eux.

On a y pair $\Rightarrow y=2k\Rightarrow y^2=4k^2=4pq\Rightarrow k^2=pq$ et comme $p\wedge q=1$ Alors p et q sont Des carrées parfaits.

3. Remarquons d'abord que si $(x,y,z)\in E$ alors $(y,x,z)\in E$ et $(kx,ky,kz)\in E$

Tenant compte de cette remarque et des questions 1. et 2. on peut conclure que

$E=\{(k(a^2-b^2),k(2ab),k(a^2+b^2))\ ;(k(2ab),k(a^2-b^2),k(a^2+b^2));\ k\in IN^*$ et $a>b>0\}$

4.

b=1 et a=2 ⟹ (3,4,5) ;(6,8,10) ; (9,12,15) ;(4,3,5); (8,6,10);(12,9,15)

b= 1 et a=3 ⟹ (8,6,10) ; (6,8,10

b=1 et a=4 ⟹ (15,8,17) ; (8,15,17) b=1 et a=5 ⟹ z>18

b=2 et a=3 ⟹ (5,12,13) ;(12,5,13)

b=2 et a=4 ⟹ z>18 b=3 et a=4 ⟹ z>18

Conclusion: Tous les triplets de E tels que z EMBED Equation.DSMT4 18 sont :
(3,4,5) ;(6,8,10) ; (9,12,15) ;(4,3,5); (8,6,10);(12,9,15); (15,8,17) ; (8,15,17)
(5,12,13) ;(12,5,13)

EX 29 :

1. a/ B→i=2⇒ $a^i=5^2=25\equiv 3(11)$ ⇒f(i)=3→C
   A→i=1⇒ $a^i=5^1=5\equiv 5(11)$ ⇒f(i)=5→E
   C→i=3⇒ $a^i=5^3=125\equiv 4(11)$ ⇒f(i)=4→D

Message	B	A	C
i	2	1	3
f(i)	3	5	4
Code	C	E	D

b/ F→i=6⇒ $a^i=5^6\equiv 5\ (11)$ ⇒f(i)=5→E
A→i=1⇒ $a^i=5^1=5\equiv 5(11)$ ⇒f(i)=5→E
D→i=4⇒ $a^i=5^4\equiv 9(11)$ ⇒f(i)=9→I
E→i=5⇒ $a^i=5^5\equiv 1\ (11)$ ⇒f(i)=1→A

Donc le message «FADE» est codé «EEIA»

On ne peut pas déchiffrer avec certitude le message codé car E peut-être déchiffrer F ou A.

2. a=2

Message	A	B	C	D	E	F	G	H	I	J
i	1	2	3	4	5	6	7	8	9	10
f(i)	2	4	8	5	10	9	7	3	6	1
Code	B	D	H	E	J	I	G	C	F	A

Oui on peut déchiffrer avec certitude un message codé (bijection)

3. a/ (⇒)

$a^{i'}\equiv a^i(11)\Leftrightarrow a^{i'}=a^i+11k\Leftrightarrow a^{i'}-a^i=11k\Leftrightarrow a^i.(a^{i'-i}-1)=11k$

$$\Rightarrow \left.\begin{array}{l} 11\left|a^i(a^{i'-i}-1)\right. \\ or\ 11\wedge a=1 \end{array}\right)\Rightarrow 11\left|a^{i'-i}-1\right.\Rightarrow a^{i'-i}\equiv 1(11)$$

(⇐) si $a^{i'-i}\equiv 1(11)\Rightarrow a^{i'-i}.a^i\equiv 1.a^i(11)\Rightarrow$

Cl :

$$a^{i'}\equiv a^i(11) \quad\Leftrightarrow\quad a^{i'-i}\equiv 1(11)$$

b/ f permet de chiffrer et de déchiffrer avec certitude tous les messages ssi $\forall i'\neq i\ \ a^{i'}\neq a^i(11)$ ssi $a^{i'-i}\neq 1(11)$ i et i' deux entiers compris entre 1 et 10 et i<i'

$\Rightarrow i'-i\in\{1,2,3,\ldots,9\}$

ssi a^i n'est pas congru à 1 modulo 11 pour tout $i\in\{1,2,3,\ldots,9\}$

c/ On a a< 11 donc 11 ne divise pas a ;et comme 11 nombre premier Alors d'après th de Fermat $a^{10}\equiv 1(11)$

Supposons que k ne divise pas 10 alors 10= n.k+u avec u<k

$a^k\equiv 1(11)\Rightarrow a^{n.k}\equiv 1(11)$ et comme $a^{10}\equiv 1(11)$ Alors $a^{10-n.k}\equiv 1(11)\Rightarrow a^u\equiv 1(11)$ avec u<k

Absurde car k est le plus petit entier deΩ tel que $a^k\equiv 1(11)$.

d/ Pour bien choisir a il suffit que a^2 et a^5 ne sont pas congrus à 1 modulo 10.

CH8 IDENTITE DE BEZOUT

EX 30 :

1. $F_0=0$; $F_1=1$; $F_2=F_1+F_0=1$; $F_3=F_2+F_1=2$; $F_4=3$; $F_5=5$
   $F_6=8$; $F_7=13$; $F_8=21$; $F_9=34$; $F_{10}=55$

2. (Par recurrence)
   *Pour n=1: $(-1)^n=(-1)^1=-1$ et $F_{n+1}F_{n-1}-F_n^2=F_2F_0-F_1^2=-1$
   Donc la proprieté est vrai à l'ordre initial.
   *Soit $n\in IN^*$ supposons que $F_{n+1}F_{n-1}-F_n^2=(-1)^n$
   et montrons que $F_{n+2}F_n-F_{n+1}^2=(-1)^{n+1}$

$$F_{n+2}F_n-F_{n+1}^2=(F_{n+1}+F_n).F_n-F_{n+1}^2=F_n^2+F_{n+1}F_n-F_{n+1}^2$$
$$=F_n^2-F_{n+1}(F_{n+1}-F_n)$$
$$=F_n^2-F_{n+1}(F_n+F_{n-1}-F_n)$$
$$=F_n^2-F_{n+1}.F_{n-1}=-(F_{n+1}F_{n-1}-F_n^2)=-(-1)^n$$
$$=(-1)^{n+1}$$

   Cl : pour tout entier non nul n on a : $F_{n+1}F_{n-1}-F_n^2=(-1)^n$

3. pour tout entier non nul n on a : $F_{n+1}F_{n-1}-F_nF_n=(-1)^n$
   et comme pour tout entier non nul n F_n est un entier ; alors d'après th de bézout $F_n\wedge F_{n+1}=1$

4. (Par recurrence sur m)
   *Pour m=0 $F_{n+m}=F_n$ et $F_mF_{n-1}+F_{m+1}F_n=F_0F_{n-1}+F_1F_n=F_n$
   Donc la proprieté est vrai à l'ordre initial
   *Soi $m\in IN$ Supposons que $F_{n+m}=F_mF_{n-1}+F_{m+1}F_n$
   Et montrons que $F_{n+m+1}=F_{m+1}F_{n-1}+F_{m+2}F_n$

$$F_{n+m+1}=F_{n+m}+F_{n+m-1}=F_mF_{n-1}+F_{m+1}F_n+F_{m-1}F_{n-1}+F_mF_n$$
$$=(F_m+F_{m-1})F_{n-1}+(F_{m+1}+f_m)F_n$$
$$=F_{m+1}F_{n-1}+F_{m+2}F_n$$

   Cl : pour tout entier non nul n et pour tout entier m on a $F_{n+m}=F_mF_{n-1}+F_{m+1}F_n$

5. $F_m\wedge F_{m+n}=F_m\wedge(F_mF_{n-1}+F_{m+1}F_n)=F_m\wedge(F_{m+1}F_n)=F_m\wedge F_n$ car $F_m\wedge F_{m+1}=1$

CH 8 IDENTITE DE BEZOUT

EX 31 :

1. Tout les entiers non nul et inférieurs à 7 sont premiers avec7donc $\varphi(7)=6$
   les entiers non nul , inférieurs à 8 et premiers avec 8 sont : 1 ;3 ;5 et 7
   donc $\varphi(8)=4$
2. Comme 0 n'est pas premier avec n ; alors il existe au plus n-1 entiers inférieurs à n et premiers avec n donc $\varphi(n)\leq n-1$
3. a/ p est premier donc tout les entiers non nul et inférieurs à p sont premiers avec p donc $\varphi(p)=p-1$
   b/ a non divisible par p et p premier alors d'après th de Fermat $a^{p-1}\equiv 1(p)$
   et comme $\varphi(p)=p-1$ alors $a^{\varphi(p)}\equiv 1(p)$
4. a/ p et q sont deux nombres premiers ;alors les nombres non premiers avec pq sont seulement les multiples de p ou les multiples de q
   Or il ya exactement q-1 multiples non nul de p inférieur à pq
   et il ya exactement p-1 multiples non nul de q inférieur à pq
   et il ya exactement pq-1 entier non nul et inférieur à pq
   Alors $\varphi(pq)= (pq-1) - [(q-1)+(p-1)]= pq-p-q+1=(p-1)(q-1)= \varphi(p).\varphi(q)$
   b/ On a $a^{\varphi(p)}\equiv 1(p)\Rightarrow (a^{\varphi(p)})^{\varphi(q)}\equiv 1(p)\Rightarrow a^{\varphi(p)\varphi(q)}\equiv 1(p)\Rightarrow a^{\varphi(pq)}\equiv 1(p)$
   On a $a^{\varphi(q)}\equiv 1(q)\Rightarrow (a^{\varphi(q)})^{\varphi(p)}\equiv 1(q)\Rightarrow a^{\varphi(q)\varphi(p)}\equiv 1(q)\Rightarrow a^{\varphi(pq)}\equiv 1(p)$
   Et comme $p\wedge q=1$
   Alors $a^{\varphi(pq)}\equiv 1(pq)$

   > Si($n\equiv 0(a)$; $n\equiv 0(b)$ et $a\wedge b=1$) Alors $n\equiv 0(ab)$

   c/ $1649=97\times 17$ (17 et 97 sont premiers ; $\varphi(17)=16$ $\varphi(97)=96$)
   10 n'est pas divisible par 17 et par 97 alors d'après b/
   $10^{16\times 96}\equiv 1(97\times 17)\Rightarrow 10^{1536}\equiv 1(1649)$
   $10403=101\times 103$ (101 et 103 sont premiers ; $\varphi(101)=100$ $\varphi(103)=102$)
   10430 n'est pas divisible par 101 et par 103 alors d'après b/
   $10430^{100\times 102}\equiv 1(101\times 103)\Rightarrow 10^{10200}\equiv 1(10403)$
5. a/ p étant premier donc seuls les multiples de p ne sont pas premiers avec p^k qui sont :1.p ;2.p ;3.p ;... ;$p^{k-1}.p=p^k$ Donc il ya $p^{k-1}-1$ entiers inférieur à p^k et non premiers avec p^k donc $\varphi(p^k)=(p^k-1)-(p^{k-1}-1)=p^k-p^{k-1}$
   b/ $\varphi(125)=\varphi(5^3)=5^3-5^2=100$;$\varphi(256)=\varphi(2^8)=2^8-2^7=128$; $\varphi(1331)=\varphi(11^3)=11^3-11^2$
6. a/ $$(1+up)^{p^{k-1}}=\sum_{j=0}^{p^{k-1}}C_{p^{k-1}}^{j}(u.p)^j=1+\sum_{j=1}^{p^{k-1}}C_{p^{k-1}}^{j}(u.p)^j$$
   et comme p^{k-1} *divise* $C_{p^{k-1}}^{j}$ *Alors* p^k *divise* $C_{p^{k-1}}^{j}(u.p)^j$ $\forall j\in\{1;2;...;p^{k-1}\}$
   b/ (Par récurrence) * Pour k=1 La propriété est vrai d'après 3. b/
   *Soit $k\in IN^*$ supposons que $a^{\varphi(p^k)}\equiv 1(p^k)\Rightarrow a^{\varphi(p^k)}=1+u.p^k$
   Et montrons que $a^{\varphi(p^{k+1})}\equiv 1(p^{k+1})$
   D'après 5. a/ on a $\varphi(p^k)=p^k-p^{k-1}\Rightarrow \varphi(p^{k+1})=p.\varphi(p^k)$
   Donc $a^{\varphi(p^{k+1})}=a^{p.\varphi(p^k)}=(a^{\varphi(p^k)})^p=(1+u.p^k)^p\equiv 1(p^{k+1})$

Pour a=17 ;p=5 et k=3 on obtient $17^{100}\equiv 1(125)$; pour a=17 ; p=2 et k=8 on obtient...